Statistics associated with reductions of elliptic curves modulo p

The University of Georgia

Paul Pollack

New approaches in probabilistic and multiplicative number theory

December 12, 2014

Introduction

Fix an elliptic curve $E/\mathbb{Q}$. We know that for each prime p of good reduction,

$$\#E(\mathbb{F}_p) = p + 1 - a_p,$$

where $|a_p| \leq 2\sqrt{p}$. Moreover,

$$E(\mathbb{F}_p) \cong \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z},$$

for uniquely determined positive integers d_p and e_p where $d_p \mid e_p$. The integers d_p and e_p are the **invariant factors** of the group.

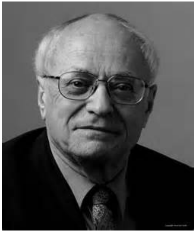
We would like to understand how the d_p and e_p behave as p varies over primes of good reduction.

A prototypical result

Question: How often is $d_p = 1$?

Theorem (Serre, 1977)

Assume GRH. Let $E/\mathbb{Q}$ be a fixed elliptic curve with an irrational 2-torsion point. Then $E(\mathbb{F}_p)$ is cyclic for a well–defined positive proportion of primes p.



If E has CM, the GRH assumption can be omitted (Murty, 1979 and Cojocaru, 2003).

Titchmarsh's divisor problem

The Titchmarsh divisor problem asks one to estimate

$$\sum_{p \leq x} \tau(p-1).$$

Under GRH, Titchmarsh (1931) showed that as $x \to \infty$,

$$\sum_{p \leq x} \tau(p-1) \sim \frac{\zeta(2)\zeta(3)}{\zeta(6)} x.$$

The assumption of GRH was eventually removed by Linnik (1963). Today, the result can be thought of as a fairly simple corollary of the Brun–Titchmarsh and Bombieri–Vinogradov results.

Titchmarsh's divisor problem

What would an analogue for elliptic curves look like?

Akbary and Ghioca (2012): Observed that $d \mid p-1 \iff p$ splits completely in $\mathbb{Q}(\zeta_d)$. Since $\mathbb{Q}(E[d])$ is analogous to $\mathbb{Q}(\zeta_d)$, an analogue of $\tau(p-1)$ would be

$$\underbrace{\sum_{d\colon\ p \text{ splits completely in } \mathbb{Q}(E[d])} 1}_{\text{in fact, this is } \tau(d_p)} .$$

Theorem

Fix an elliptic curve $E/\mathbb{Q}$. As $x \to \infty$, we have $\sum_{p \le x} \tau(d_p) \sim c_E \pi(x)$. Here GRH is assumed unless E has CM.

Of course, one could be more naive about the analogue one considers.

What about just $\sum_{p \le x} \tau(\# E(\mathbb{F}_p))$?

Theorem (P.)

Fix $E/\mathbb{Q}$. If E has CM, then $\sum_{p \le x} \tau(d_p e_p) \sim c_E x$, as $x \to \infty$, where c_E is a positive constant depending on E.

Of course, one could be more naive about the analogue one considers.

What about just $\sum_{p\le x}\tau(\#E(\mathbb{F}_p))$?

Theorem (P.)

Fix $E/\mathbb{Q}$. If E has CM, then $\sum_{p\le x}\tau(d_p e_p)\sim c_E x$, as $x\to\infty$, where c_E is a positive constant depending on E.

If we do not assume E has CM, but do assume GRH, $\sum_{p\le x}\tau(d_p e_p)\asymp x$.

The Akbary–Ghioca result has been extended by Felix and Murty (2013) to estimate other sums of the form

$$\sum_{p \leq x} f(d_p).$$

They assume one can write $f = \sum_{d|n} g(d)$ where $\sum_{d \leq x} |g(d)|$ is appropriately bounded.

Example

Assume $E/\mathbb{Q}$ is an elliptic curve with CM. Fix $0 < \alpha < 1$. As $x \to \infty$,

$$\sum_{p \leq x} d_p^{\alpha} \sim c_{E,\alpha} \cdot \pi(x),$$

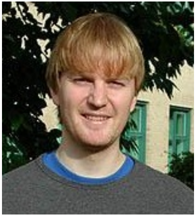
where $c_{E,\alpha} > 0$.

The last example suggests studying the mean value of d_p, and also of e_p.

Information about these mean values should encode how near to cyclic $E(\mathbb{F}_p)$ is, on average.

The last example suggests studying the mean value of d_p, and also of e_p.

Information about these mean values should encode how near to cyclic $E(\mathbb{F}_p)$ is, on average.

Theorem (Freiberg–Kurlberg, 2014)

Fix $E/\mathbb{Q}$. Then as $x \to \infty$, $\sum_{p \le x} e_p \sim c_E \frac{x^2}{\log x}$, for some $c_E > 0$. GRH is assumed if E does not have CM.

Theorem (Freiberg–Kurlberg, 2014)

Fix $E/\mathbb{Q}$. As $x \to \infty$, $\sum_{p \le x} e_p \sim c_E \frac{x^2}{\log x}$, for some $c_E > 0$. GRH is assumed if E does not have CM.

Since also $\sum_{p \le x} p \asymp \frac{x^2}{\log x}$, we see that e_p is of average order $\mathrm{const} \cdot p$.

Theorem (Freiberg–Kurlberg, 2014)

Fix $E/\mathbb{Q}$. As $x \to \infty$, $\sum_{p \le x} e_p \sim c_E \frac{x^2}{\log x}$, for some $c_E > 0$. GRH is assumed if E does not have CM.

Since also $\sum_{p \le x} p \asymp \frac{x^2}{\log x}$, we see that e_p is of average order $\text{const} \cdot p$.

Since $d_p e_p = p + 1 - a_p \sim p$, this suggests that d_p is usually bounded.

Theorem (Duke, 2003)

Let $\psi(p)$ be any function that tends to ∞. Then $d_p < \psi(p)$ for almost all primes p. GRH is assumed if E does not have CM.

Duke's result tells us about the normal order of d_p. What about the average order?

Question

What is the asymptotic behavior of $\sum_{p \le x} d_p$?

Duke's result tells us about the normal order of d_p. What about the average order?

Question

What is the asymptotic behavior of $\sum_{p \le x} d_p$?

This question was proposed by Kowalski (2001), who conjectured that

$$\begin{aligned} \sum_{p \le x} d_p &\sim c_E \pi(x) && \text{if } E \text{ does not have CM} \\ &\sim c_E x && \text{if } E \text{ has CM.} \end{aligned}$$

If E does not have CM, there has been very little progress towards the upper bound; e.g., even on GRH, $x^{1+o(1)}$ is unknown (to me).

Suppose $E/\mathbb{Q}$ is a fixed elliptic curve with CM. Then

$$x\frac{\log\log x}{\log x} \ll \sum_{p\leq x} d_p \ll x\sqrt{\log x} \qquad \text{(Kowalski, 2001)}$$

$$\sum_{p\leq x} d_p \ll x\log\log x \qquad \text{(Kim, 2014).}$$

Kowalski's argument was fleshed out by Felix and Murty (2013), who noted a small improvement:

$$\frac{\sum_{p\leq x} d_p}{x\log\log x/\log x} \to \infty.$$

Suppose $E/\mathbb{Q}$ is a fixed elliptic curve with CM. Then

$$x\frac{\log\log x}{\log x} \ll \sum_{p\le x} d_p \ll x\sqrt{\log x} \qquad \text{(Kowalski, 2001)}$$

$$\sum_{p\le x} d_p \ll x\log\log x \qquad \text{(Kim, 2014).}$$

Kowalski's argument was fleshed out by Felix and Murty (2013), who noted a small improvement:

$$\frac{\sum_{p\le x} d_p}{x\log\log x/\log x} \to \infty.$$

Theorem (Freiberg and P., 2014)

For large x, we have $\sum_{p\le x} d_p \asymp x$.

Part II: Proofs

The average number of divisors of $\#E(\mathbb{F}_p)$

Fix an elliptic curve $E/\mathbb{Q}$ without CM. We claimed that on GRH,

$$\sum_{p \le x} \tau(\#E(\mathbb{F}_p)) \asymp x.$$

To prove this, one would like to write $\tau(\cdot) = \sum_{d|\cdot} 1$, and to reverse the order:

$$\sum_{d \le 2x} \#\{p \le x : d \mid \#E(\mathbb{F}_p)\}.$$

The average number of divisors of $\#E(\mathbb{F}_p)$

Fix an elliptic curve $E/\mathbb{Q}$ without CM. We claimed that on GRH,

$$\sum_{p \le x} \tau(\#E(\mathbb{F}_p)) \asymp x.$$

To prove this, one would like to write $\tau(\cdot) = \sum_{d|\cdot} 1$, and to reverse the order:

$$\sum_{d \le 2x} \#\{p \le x : d \mid \#E(\mathbb{F}_p)\}.$$

The summand can be understood for $d < x^{1/10}$. This is enough to get a lower bound.

To get an upper bound, one has to replace the sum over all divisors with a quantity sensitive only to *small divisors*.

Theorem

Uniformly for $n \le x$,

$$\tau(n) \ll_\theta \sum_{\substack{d|n \\ d \le x^\theta}} 1 + \sum_{r \ge 1} M_r \sum_{\substack{d|n \\ x^{\theta/4} < d \le x^\theta \\ p|d \Rightarrow p \le x^{1/r}}} 1,$$

where

$$M_r = \min\{2^{r+1}, \exp(\log x / \log\log x)\}.$$

A majorant of this kind first appears in 1952 work of Erdős (see also Wolke, Shiu, Tao, ...).

Substituting in this majorant, reversing the order of summation, using the David–Wu bound, and using standard results on the distribution of smooths, we eventually find that

$$\sum_{p \le x} \tau(\#E(\mathbb{F}_p)) \ll x,$$

as claimed.

The average of the first invariant factor mod p

Recall our claim that for CM curves,

$$\sum_{p \le x} d_p \asymp x.$$

For simplicity, **the** CM curve is

$$E: \ y^2 = x^3 - x,$$

which has CM by the ring of Gaussian integers $\mathbb{Z}[i]$.

For the primes $p \equiv 3 \pmod 4$,

$$\#E(\mathbb{F}_p) = p + 1.$$

These are the **supersingular primes.** For these $d_p \le 2$, and so these can be ignored.

Suppose instead that $p \equiv 1 \pmod 4$. These are our **ordinary primes**. Then p factors in $\mathbb{Z}[i]$ as

$$p = \pi\bar{\pi},$$

where $\pi \equiv 1 \pmod{(1+i)^3}$. (In other words, π is **primary**.)

Then

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \bar{\pi}) = N(\pi - 1),$$

and if we write $\pi = a_p + b_p i$, then

$$d_p = \gcd(a_p - 1, b_p)$$

Using the identity $d_p = \sum_{d \mid d_p} \phi(d)$, and remembering that $d_p^2 \mid d_p e_p = \#E(\mathbb{F}_p) \leq (\sqrt{x}+1)^2$, we have

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod 4}} d_p = \sum_{\substack{p \leq x \\ p \equiv 1 \pmod 4}} \sum_{d \mid d_p} \phi(d)$$

$$= \sum_{d \leq \sqrt{x}+1} \phi(d) \sum_{\substack{p \leq x \\ p \equiv 1 \pmod 4 \\ d \mid d_p}} 1$$

$$= \frac{1}{2} \sum_{d \leq \sqrt{x}+1} \phi(d) \sum_{\substack{N(\pi) \leq x \\ N(\pi) \text{ prime}, \equiv 1 \pmod 4 \\ \pi \equiv 1 \pmod{[d, (1+i)^3]}}} 1.$$

OK, so

$$\sum_{\substack{p\leq x\\ p\equiv 1 \pmod 4}} d_p = \frac{1}{2}\sum_{d\leq\sqrt{x}+1}\phi(d) \sum_{\substack{N(\pi)\leq x\\ N(\pi) \text{ prime}, \equiv 1 \pmod 4\\ \pi\equiv 1 \pmod{[d,(1+i)^3]}}} 1.$$

Let's look at the **upper bound**.
If we use Brun–Titchmarsh for $\mathbb{Z}[i]$, the inner sum is

$$\ll \frac{x}{\Phi(d)\log\frac{4x}{d^2}},$$

where Φ is the Euler function for $\mathbb{Z}[i]$.

Using this above and summing, we are led to Kim's bound

$$\ll x\log\log x.$$

To avoid losing a $\log\log$ factor, we need to treat the d close to $\sqrt{x}$ more efficiently.

The part of the sum corresponding to $d \leq x^{1/3}$ is OK, by the above argument, since then $\log \frac{4x}{d^2} \asymp \log x$. So suppose $d > x^{1/3}$.

We now have to estimate

$$\sum_{x^{1/3} < d \leq \sqrt{x}+1} \phi(d) \sum_{\substack{N(\pi) \leq x \\ N(\pi) \text{ prime}, \equiv 1 \pmod 4 \\ \pi \equiv 1 \pmod{[d, (1+i)^3]}}} 1.$$

In the inner sum, write $\pi = \omega d + 1$. If $N(\pi) \leq x$, then $N(\omega) \leq 4\sqrt{x}/d$. If $N(\omega d + 1)$ is prime, clearly $\mathrm{Im}(\omega) \neq 0$.

We invert the order of summation and after some simplifications, we are left with the problem of bounding

$$\sum_{\substack{N(\omega)\leq 4\sqrt{x} \\ \mathrm{Im}(\omega)\neq 0}} \sum_{\substack{x^{1/3}<d\leq 4\sqrt{x}/N(\omega) \\ N(\omega d+1) \text{ prime}}} \phi(d).$$

Replace $\phi(d)$ with $4\sqrt{x}/N(\omega)$.
The problem comes down to counting $d \in (x^{1/3}, 4\sqrt{x}/N(\omega)]$ for which the quadratic polynomial

$$N(\omega d + 1) = N(\omega)d^2 + Tr(\omega)d + 1$$

is prime.

The upper bound sieve gives that this is

$$\ll \mathfrak{S}\frac{\sqrt{x}/N(\omega)}{\log x},$$

where $\mathfrak{S}$ is a certain singular series depending on the particular quadratic polynomial.

(We can assume $4\sqrt{x}/N(\omega) > x^{1/3}$. This is why we get a denominator proportional to $\log x$.)

If $\mathfrak{S}$ were 1, we could sum with no problems. To complete the proof, one shows $\mathfrak{S}$ averages to $\ll 1$ in a suitable sense. Here mean value theorems for nonnegative multiplicative functions are used.

What about the lower bound?

Remember, we need to bound from below

$$\frac{1}{2}\sum_{d\leq\sqrt{x}+1}\phi(d)\sum_{\substack{N(\pi)\leq x\\ N(\pi)\text{ prime},\equiv 1\pmod 4\\ \pi\equiv 1\pmod{[d,(1+i)^3]}}} 1.$$

One's first inclination is to truncate the sum on d use Bombieri–Vinogradov; but the weights $\phi(d)$ complicate matters.

One can carry this out with a **severe** truncation, going only up to $(\log x)^A$, and use B–V to get $\gg x\log\log x/\log x$ (Felix and Murty), with an arbitrarily large implied constant.

Rather than try to bound

$$\frac{1}{2}\sum_{d\le\sqrt{x}+1}\phi(d)\sum_{\substack{N(\pi)\le x\\ N(\pi)\text{ prime},\equiv 1 \pmod 4\\ \pi\equiv 1 \pmod{[d,(1+i)^3]}}} 1$$

from below using an average result, we use a result about **most** individual progressions.

Specifically, using work of Weiss — who proved a generalization of Linnik's theorem for algebraic number fields — we show that if d is not divisible by a certain exceptional modulus, then we get a lower bound on the inner sum of the correct order for d up to some small power of x. This is enough.

Under construction

There is a third variant of the Titchmarsh divisor problem one could consider (suggested to us by Greg Martin): View $\tau(p-1)$ as counting the number of subgroups of $\mathbb{F}_p^\times$.

If $s(G)$ denotes the number of subgroups of G, one could ask for an estimate of

$$\sum_{p \le x} s(E(\mathbb{F}_p)).$$

In work in progress with Freiberg, we hope to show that when E has CM, this sum is $\asymp x \log x$, for large x.

The starting point is the beautiful formula

$$s(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \sum_{d|m,\ e|n} \gcd(d, e).$$

(Calhoun, 1987.)

Estimating the average of $s(\#E(\mathbb{F}_p))$ appears to require a hybrid of the techniques used to study the average of $\tau(d_p e_p)$ and the average of d_p.

Thank you!